Richard Dedekind and the development of the theory of finite fields

Niederreiter, Harald

Veröffentlicht in:
Abhandlungen der Braunschweigischen
Wissenschaftlichen Gesellschaft Band 33, 1982,
S.183-187

Verlag Erich Goltze KG, Göttingen

Richard Dedekind and the development of the theory of finite fields

By **Harald Niederreiter***, Frankfurt

In the years 1856–57 the young Privatdozent Dedekind followed Dirichlet's lectures on number theory at the University of Göttingen which he later was to edit in such masterly form. It is certainly safe to say that this experience turned out to be decisive for Dedekind's mathematical career. Dirichlet had just come from Berlin to Göttingen, where he succeeded Gauss, and brought with him a dazzling collection of new techniques and concepts in analytic and algebraic number theory which immediately fascinated his pupil. The arrival of Dirichlet could not have come at a better time since Dedekind seems to have been searching for a subject on which to focus his talents. Several years ago he had abandoned Euler integrals, the topic of his dissertation under the direction of Gauss, and in the meantime he had dabbled without any noteworthy success in analytic geometry and elementary probability theory. The systematic exposure to a field like number theory, which was at an exciting stage of its development following the progress achieved by Dirichlet, Kummer, Eisenstein, Jacobi, and Cauchy in the previous two decades, just provided the impetus he needed.

One of the consequences of Dedekind's involvement with Dirichlet's lectures was his observation that Gauss's project of developing a theory of "higher congruences" (see [10]) could be carried out by establishing an analogy with the theory of ordinary congruences and then emulating Dirichlet's approach to the latter topic. The most important outgrowth of this observation is the seminal paper [6] which not only put the theory of "higher congruences" (or, equivalently, of finite fields) on a sound basis, but also played a role in the conceptual development of algebraic number theory and abstract algebra. Moreover, the results of this paper were used later by Dedekind in his famous work on the factorization of ideals in rings of algebraic integers.

The basic properties of the finite prime fields $F_p = \mathbb{Z}/p\mathbb{Z}$ were already established well before Dedekind's time through the efforts of Fermat, Euler, Lagrange, Legendre, and Gauss. The next step in the genesis of the theory of finite fields was the investigation of the arithmetic in the polynomial rings $F_p[x]$, in particular the realization that in these rings the Euclidean algorithm and unique factorization are valid. This was carried out with admirable precision by Gauss in his posthumous paper [10] which, as the introduction to [6] suggests, was known to Dedekind. The construction of extension fields of F_p was described by Galois [9], who used an "imaginary" root i

* This work was carried out while the author was supported by the Alexander von Humboldt-Stiftung.

of an irreducible polynomial over F_p of degree n and showed that the expressions $a_0 + a_1 i + \ldots + a_{n-1} i^{n-1}$ with $a_j \in F_p$ form a field of order p^n. This process was regarded with some suspicion by Gauss (see [10], § 338), and in fact our modern standpoint would only allow this construction if i is contained in some a priori given extension of F_p. Gauss adds in a footnote: "Vielleicht werden wir bei anderer Gelegenheit unsere Ansicht hierüber ausführlicher darlegen", but he never returned to the subject.

Another contribution to the theory of finite fields prior to Dedekind's work is that of Schönemann [17]. Here the use of imaginary roots is avoided by employing complex roots obtained from the fundamental theorem of algebra. This is again not entirely satisfactory. An interesting technical innovation is the use of double modulus congruences for setting up equivalence relations among polynomials. For $f,g,h \in \mathbb{Z}[x]$ and a complex root α of f, Schönemann writes $g \equiv h \pmod{p,\alpha}$ if $g(\alpha) = h(\alpha) + pr(\alpha)$ for some $r \in \mathbb{Z}[x]$.

It should be noted that shortly before Dedekind started to write about finite fields, Serret brought out the second edition of his widely read book [18] on higher algebra which included an account of the results of Galois and some of his own ideas, so that Dedekind was certainly familiar with the work of all his predecessors both in Germany and in France.

In his paper [6] Dedekind's first important observation is the close analogy between the arithmetic in $\mathbb{Z}$ and the arithmetic in $F_p[x]$. He proves again the results of Gauss [10] on greatest common divisors and unique factorization in $F_p[x]$ by modeling the arguments on the corresponding ones for $\mathbb{Z}$. Polynomials over F_p are viewed as equivalence classes of polynomials over $\mathbb{Z}$ in an obvious way.

A major novelty in [6] is a rigorous construction of finite fields of order p^n for which the objections against earlier constructions do not apply. Dedekind's idea evolves from the systematic extension of the theory of congruences to the ring $F_p[x]$. This is achieved by means of double modulus congruences in the following sense. If $A, B, M \in \mathbb{Z}[x]$, then Dedekind writes $A \equiv B$ (modd. p,M), or briefly $A \equiv B$ (mod. M), if $A - B$ is divisible modulo p by M. He shows that a complete system of incongruent polynomials (with respect to this double modulus congruence) contains exactly p^n elements, where n is the degree of M modulo p. If M is taken to be an irreducible polynomial P modulo p, then it is proved that such a complete system forms a field. In modern terms, finite fields of order p^n are constructed as residue class rings $F_p[x]/(P)$ with $P \in F_p[x]$ irreducible of degree n. Since it is also shown in the paper that for every positive integer n there is an irreducible $P \in F_p[x]$ of degree n (which is, in fact, a consequence of the formula of Gauss [10] for the number of monic irreducible polynomials over F_p of fixed degree), it follows that Dedekind knew how to construct finite fields for any prime-power order in a rigorous manner. It was only shown much later by Moore [13], [14] that finite fields must have primer-power orders and that finite fields of the same prime-power order are isomorphic. Therefore, Dedekind's construction yields all possible finite fields.

Dedekind's use of double modulus congruences is somewhat awkward from a modern standpoint, but he displays considerable ease in working with the resulting

equivalence classes. The structure of the residue class rings $F_p[x]/(M)$ emerges clearly from his investigation. With several epochs of abstract algebra between us and the early masters, it is of course a triviality to observe that the approach of Galois via imaginary roots and that of Dedekind via residue class rings $F_p[x]/(P)$ are essentially equivalent, although Galois's construction was not well founded at that time. The link is provided by the later result of Kronecker [11] to the effect that for any irreducible polynomial f over any field F there is an extension field of F in which f has a root. In the modern proof of this result the extension field is constructed by means of the factor ring F[x]/(f), and here we are again entering the circle of Dedekind's ideas.

The paper [6] contains a host of other results on the rings $F_p[x]$ and $F_p[x]/(M)$, but we will discuss only those which we find of interest for the history of algebra and number theory. Dedekind devotes considerable attention to the structure of the group of units of $F_p[x]/(M)$. He determines its order, thus obtaining an analog of Euler's totient function which was studied later by other authors (see e. g. Carlitz [3], [5]). He shows also that the group of units is cyclic in case M is irreducible over F_p, hence the existence of primitive elements for any finite field.

Dedekind treats also congruences of the form $G(y) \equiv 0 \pmod{P}$ with G a polynomial over $F_p[x]$ and P irreducible over F_p. In modern terminology this amounts to considering equations over the finite field of order p^n, where n is the degree of P. He proves that the number of solutions cannot exceed the degree of G. Criteria for solvability are established in the case of binomial congruences $y^k \equiv A \pmod{P}$. In the special case $k = 2$ this leads to a theory of quadratic residues and a law of quadratic reciprocity for $F_p[x]$. In detail, if Q and R are distinct monic irreducible polynomials over F_p of degree m and n, respectively, then it is shown that

$$\left(\frac{Q}{R}\right)\left(\frac{R}{Q}\right) = \left(\frac{-1}{p}\right)^{mn},$$

where the symbol on the right-hand side is the standard Legendre symbol. Such reciprocity laws were considered further by Artin [2], Carlitz [3], [4], Ore [15], and Schmidt [16]. It is an interesting phenomenon that higher reciprocity laws are easier to establish for $F_p[x]$ than for $\mathbb{Z}$.

There is an unexpected treasure hidden in [6], namely the first general statement and proof of the formula (nowadays called the Moebius inversion formula) which allows us to recover an arithmetic function from its summatory function. As an application, Dedekind finds that the number A_n of monic irreducible polynomials over F_p of degree n is given by

$$(1) \qquad A_n = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d,$$

where μ is the Moebius function. The same formula was obtained by Gauss [10], but he did not deduce it from a general inversion formula. Dedekind establishes also the multiplicative form of the Moebius inversion formula and applies it as follows. He shows the identity

$$x^{p^n} - x = \prod f(x),$$

where $f(x)$ runs through all monic irreducible polynomials over F_p of degree dividing n, and then by Moebius inversion he concludes that the product I_n of all monic irreducible polynomials over F_p of degree n is given by

$$(2) \qquad I_n = \prod_{d|n} (x^{p^d} - x)^{\mu(n/d)}.$$

This formula is still known as Dedekind's formula in the theory of finite fields (see Albert [1]). A comparison of degrees in (2) obviously yields again the formula (1).

Dedekind returned to the subject of finite fields in his fundamental paper [7] on the factorization of ideals in algebraic number fields. If K is an algebraic number field and p a rational prime, then he starts from the observation that a congruence modulo p in the ring of algebraic integers in K is equivalent to a double modulus congruence with moduli p and f, where f is an irreducible defining polynomial of K. This relationship enables him to apply results on finite fields from the earlier paper [6]. The most important application occurs in connection with the problem of factoring the principal ideal (p) of the ring of algebraic integers in K. Here f is viewed as a polynomial over F_p, and then Dedekind establishes the well-known relationship between the canonical factorization of f over F_p and the factorization behavior of the ideal (p). For the special case of cyclotomic fields this was already shown by Kummer [12]. Dedekind's proof makes essential use of properties of finite fields (or "higher congruences" in his terminology).

In one of his supplements to Dirichlet's Vorlesungen, Dedekind reviews briefly the connection between double modulus congruences and congruences modulo prime ideals in algebraic number fields, and he remarks also that in the theory developed in [6] the underlying field F_p can be replaced by any finite field (see [8], § 180). Thus, Dedekind's method allows the treatment of extensions of finite fields in full generality.

We have already noted in several instances the influence of Dedekind's work on later developments. A mathematician who acknowledged his special indebtedness to Dedekind was Emil Artin. In his pioneering paper [2] on algebraic function fields with finite fields of constants and on congruence zeta-functions, Artin was very much inspired by Dedekind's work on "higher congruences" and he followed [6] at some length in laying the foundations of his subject. Thus it seems that Dedekind's contributions to the theory of finite fields, though not on the same footing with his celebrated work on ideal theory and on the real number system, still deserve to be widely known.

References

[1] A. A. Albert, Fundamental Concepts of Higher Algebra, Univ. of Chicago Press, Chicago, 1956.

[2] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen, Math. Z. 19, 153–246 (1924); Collected Papers, pp. 1–94, Addison-Wesley, Reading, Mass., 1965.

[3] L. Carlitz, The arithmetic of polynomials in a Galois field, Amer. J. Math. 54, 39–50 (1932).
[4] L. Carlitz, On a theorem of higher reciprocity, Bull. Amer. Math. Soc. 39, 155–160 (1933).
[5] L. Carlitz, Some topics in the arithmetic of polynomials, Bull. Amer. Math. Soc. 48, 679–691 (1942).
[6] R. Dedekind, Abriß einer Theorie der höheren Congruenzen in Bezug auf einen reellen Primzahl-Modulus, J. reine angew. Math. 54, 1–26 (1857); Gesammelte Math. Werke, vol. 1, pp. 40–66, Vieweg, Braunschweig, 1930.
[7] R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Abh. Königl. Gesellschaft der Wissenschaften Göttingen 23, 1–23 (1878); Gesammelte Math. Werke, vol. 1, pp. 202–230, Vieweg, Braunschweig, 1930.
[8] R. Dedekind, Über die Theorie der ganzen algebraischen Zahlen, Supplement of Dirichlet's "Vorlesungen über Zahlentheorie", 4th ed., pp. 434–657, Vieweg, Braunschweig, 1894; Gesammelte Math. Werke, vol. 3, pp. 1–222, Vieweg, Braunschweig, 1932.
[9] E. Galois, Sur la théorie des nombres, Bull. Sci. Math. de M. Férussac 13, 428–435 (1830); Oeuvres mathématiques, pp. 15–23, Gauthier-Villars, Paris, 1897.
[10] C.F. Gauss, Analysis residuorum: Disquisitiones generales de congruentiis, Werke, vol. 2, pp. 212–240, Königl. Gesellschaft der Wissenschaften, Göttingen, 1876.
[11] L. Kronecker, Ein Fundamentalsatz der allgemeinen Arithmetik, J. reine angew. Math. 100, 490–510 (1887); Werke, vol. 3, part 1, pp. 209–240, Teubner, Leipzig, 1899.
[12] E.E. Kummer, Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren, J. reine angew. Math. 35, 327–367 (1847); Collected Papers, vol. 1, pp. 211–251, Springer-Verlag, Berlin–Heidelberg–New York, 1975.
[13] E.H. Moore, A doubly-infinite system of simple groups, Bull. New York Math. Soc. 3, 73–78 (1893).
[14] E.H. Moore, A doubly-infinite system of simple groups, Math. Papers read at the Congress of Mathematics (Chicago, 1893), pp. 208–242, Chicago, 1896.
[15] O. Ore, Contributions to the theory of finite fields, Trans. Amer. Math. Soc. 36, 243–274 (1934).
[16] F.K. Schmidt, Zur Zahlentheorie in Körpern von der Charakteristik p, Sitzungsber. Phys. Ges. Erlangen 58/59, 159–172 (1928).
[17] T. Schönemann, Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reelle Primzahl ist, J. reine angew. Math. 31, 269–325 (1846).
[18] J.A. Serret, Cours d'algèbre supérieure, 2nd ed., Mallet-Bachelier, Paris, 1854.